Certia: Certifying Interface Automata for Cyber-Physical Systems

Cong Sun, Qingsong Yao, and Jianfeng Ma

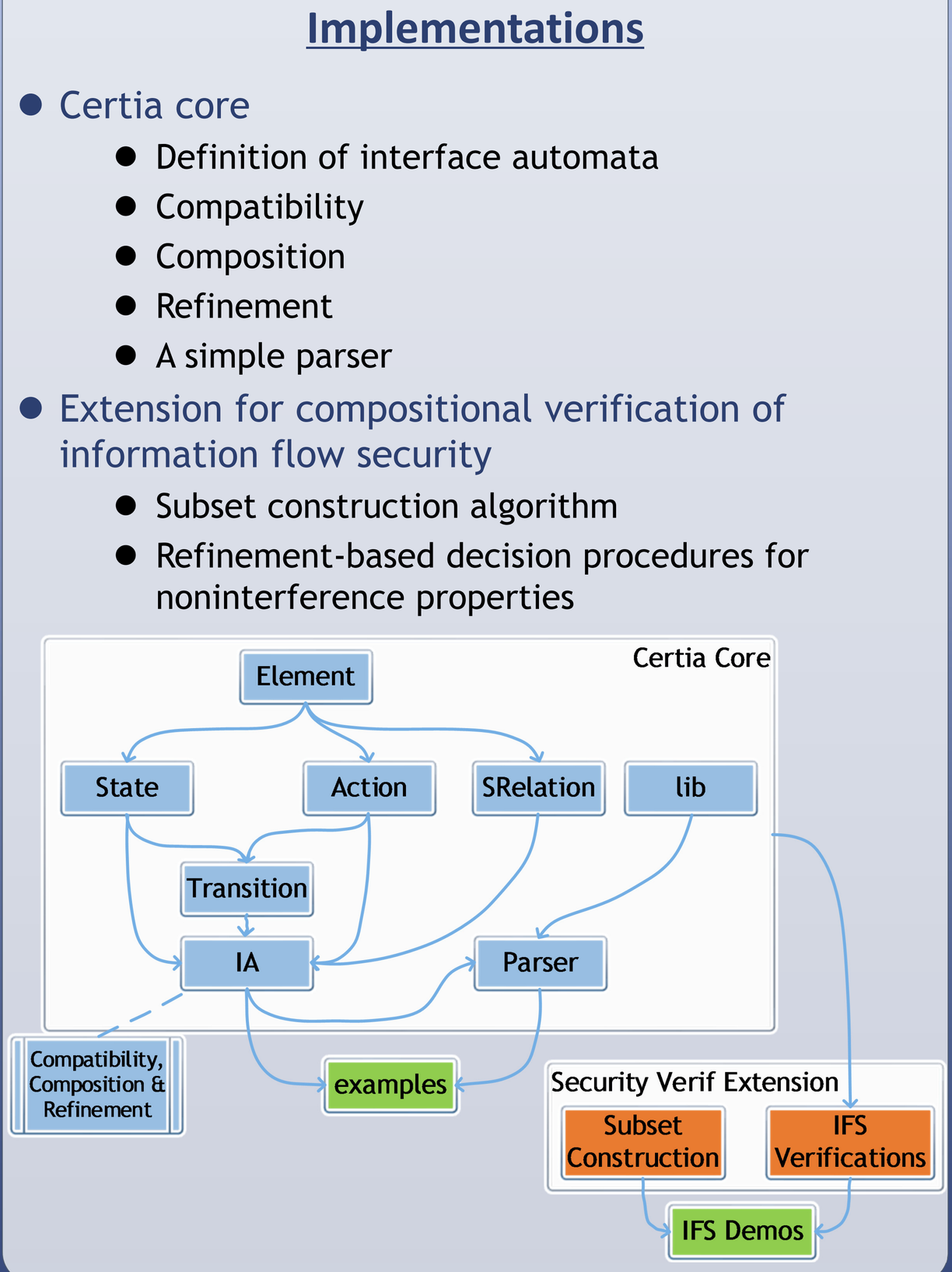
School of Cyber Engineering, Xidian University

Background & Introduction

- Component-based software development is widely considered as a promising approach on the design, and development of cyber-physical systems
- Components cooperate with each other via interfaces
  - Rigorous automaton-based interface models: I/O Automata, Component-Interaction Automata, Interface Automata, etc.
  - Impl. & tools: CHIC, TICC, Ptolemy II, etc.
- Interface automaton: Light-weighted automata-theoretic formalism capturing temporal behaviors of component-based systems
- **Contributions of this work**
  - A Coq-library of interface automata in purpose of certifying security properties of component-based CPS
  - Applications on compositional verification of information flow security for cyber-physical applications

Implementations

- Certia core
  - Definition of interface automata
  - Compatibility
  - Composition
  - Refinement
  - A simple parser
- Extension for compositional verification of information flow security
  - Subset construction algorithm
  - Refinement-based decision procedures for noninterference properties



Results & More Demos

- Demos on Composition

TABLE I
ANALYSIS RESULTS

No.	Origin	C_1	C_2	$C_1 \otimes C_2$		$C_1 \| C_2$	
				$\sharp S$	$\sharp T$	$\sharp S$	$\sharp T$
1	[2, Fig.1]	User	Comp	7	8	6	7
2	[2, Fig.4]	@1	Channel	8	10	-	-
3	[18, Fig.2]	Buf	Recv	6	9	3	3
4	[9, Fig.1]	Prod	Pay	10	14	9	13
5	[9, Fig.4]	Prod	GenPay	10	15	10	15
6	[11, Fig.1]	TS	TPU	11	15	7	10
7	[11, Fig.1]	@6	Sup	24	32	11	14
8	[4, b–f]	CtrlU	FireD1	4	3	4	3
9	[4, b–f]	@8	FireD2	6	6	6	6
10	[4, f–d]	CtrlU	FireD1	8	9	-	-
11	[4, f–d]	FireD1	FireD2	9	22	9	22
12	[4, f–d]	CtrlU	@11	22	34	22	34

- Demos on compositional verification of information flow security

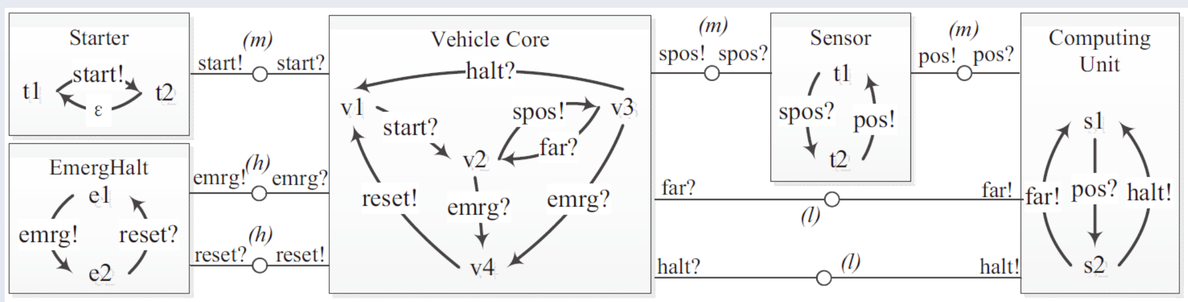
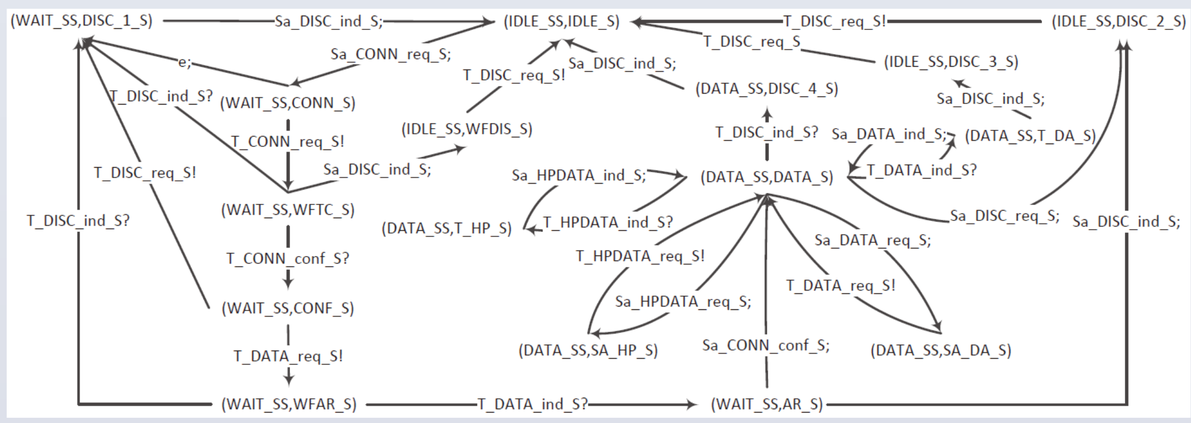
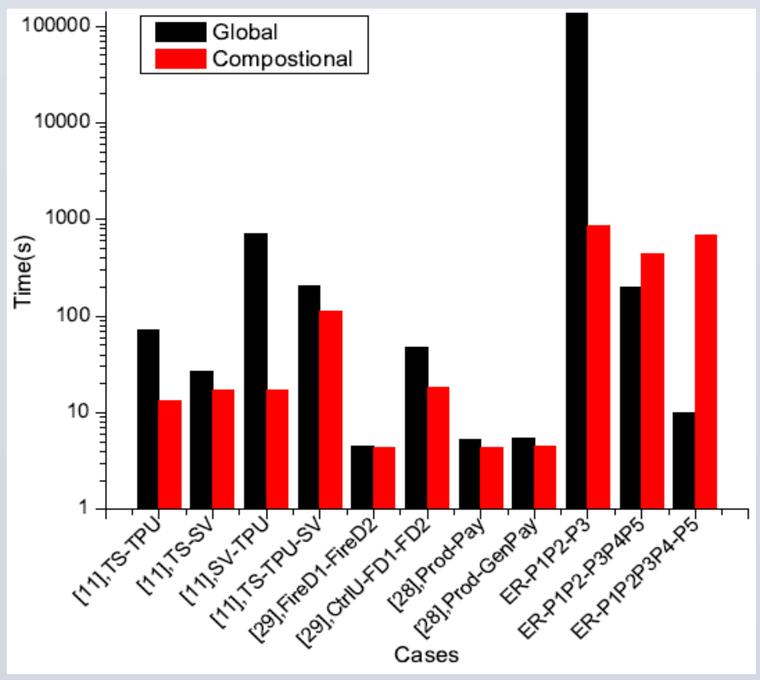


Figure 3. The interface automata of the CyCab components



- 98.4% cost reduction by compositional verification



Acknowledgements

- National High Technology Research and Development Program (863 Program) of China (No. 2015AA017203).
- National Natural Science Foundation of China (No. 61303033).
- Natural Science Basis Research Plan in Shaanxi Province of China (No. 2016JM6034).